

Mitigating the Integrity Issues in Cloud Computing Utilizing Cryptography Algorithms

Dr. Satinderjeet Singh

Associate - Cyber, Risk and Regulatory, PricewaterhouseCoopers (PwC), New York, USA. Email: drsatinderjetsingh@gmail.com

DOI: <http://doi.org/10.46382/MJBAS.2021.5208>

Copyright: © 2021 Dr. Satinderjeet Singh. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Article Received: 29 March 2021

Article Accepted: 31 May 2021

Article Published: 30 June 2021

ABSTRACT

The cloud can be created, monitored, and disseminated with slight disruption or service provider involvement. Among the most rapidly evolving phenomenon, cloud computing provides users with a variety of low-cost solutions. By putting the ideas of confidentiality, authentication, encryption techniques, non-repudiation, intrusion prevention, and effectiveness into practice, the challenge of cloud information security for computers and cloud storage security has been resolved in its totality. As cloud security has become a growing problem, cloud technology is prominent throughout many emerging disciplines of study in which a significant amount of research is conducted in this field. Each of these efforts uses a cryptography approach. Current solutions to these issues have certain important drawbacks. To protect sensitive information stored in the cloud, one needs to design programs that implement hybrid cryptographic mechanisms using challenging encryption algorithms. This research elaborates on an examination of using cryptographic techniques to mitigate the integrity problems in cloud computing.

Keywords: Cloud computing, Cryptography algorithms, Integrity issues, Intrusion detection.

1. Introduction

The major advancements in information technology and computation over the previous three decades have enabled the technology world to envision a move to the cloud technology era, which began nowadays. A powerful infrastructure of servers and information center storage, improvements in increased and scalable computing technologies for computer servers and the Internet, the building of the Internet infrastructure, the widespread use of wireless Internet connectivity, etc., are only a few examples of the advancements.

Cloud serves as an example of a decentralized network with several virtual servers that are continuously provided to meet a customer's unique resource requirements [1-3]. The entire framework of this cloud-customer cooperation is governed by the Service level agreement (SLA). The NIST has been described as an example of simple internet connectivity to a computer system that may be customized, including servers, records, programs, software, etc [4]. There are three techniques to safeguard open cloud services using cryptographic techniques [5-8].

- (1) To convert the plaintext into ciphertext, symmetric key techniques and asymmetric key techniques were used.
- (2) By substituting any other element, integer, or symbol for a direct textual character, substitution procedures can convert the plaintext into ciphertext.
- (3) The transpositional methods are employed to protect the actual text through permutations. The confidentiality and integrity of information stored in public clouds are upheld by cryptographic methods. Only the intended recipient and the sender can share data when it is private.

It guarantees that the transmitter needs these methods to ensure that the receiver is the only one who can identify the data and nobody else who is not trustworthy can. Data integrity is ensured for information stored on the cloud platform. Illegal activities are prevented from accessing inaccurate or pirated data, as well as a large number of

perspectives, and the cloud-based storage service provider upholds data integrity and accuracy. Accessibility guarantees that customers can get the networks, programs, and data they require.

According to International Data Corporation (IDC), the third quarter of 2016 saw an 8.1% growth in the profitability of cloud infrastructure products such as servers, cloud infrastructure storage, and private clouds, bringing the total to \$8.4 billion. With a yearly increase of \$53.1 billion by 2019 and \$203.4 billion globally, public clouds will outpace global IT cost growth by a factor of seven. Amazon, Google, Microsoft, and other companies are moving swiftly in developing the platforms for cloud computing and expanding the infrastructure for a sizable number of consumers. Several additional businesses, like MediaTemple, Mosso, Joyent, and others, are motivated to enter the cloud by the popularity of these businesses. Three service models—SaaS, PaaS, and IaaS—are used in cloud technology to offer customers infrastructure, platforms, programs, and software as a service. Users that use SaaS run their apps on the cloud platform companies' servers. These programs are accessible to users through internet browsers. The PaaS service delivery platforms enable users to rent their software system or to develop and test new models using resources, operating systems, storage, and networks. With the help of the IaaS, customers may manage how memory, networks, and other computing resources are used to run any program.

As cloud protection has become an increasingly important subject, cloud technology is a topic that is covered mostly in developing disciplines of study. Each of these studies used a cryptography approach. To address these issues, current techniques possess considerable drawbacks. Given that some applications should be created and execute hybrid encryption mechanisms using challenging cryptographic techniques, one should figure out a solution to safeguard sensitive information stored in the cloud. If one combines different cryptographic algorithms, according to experts, security measures would increase.

Many experts suggested hybrid cryptographic techniques since the traditional encryption schemes are insufficient for the current level of online information security. It is a method of designing data transmission that combines at least one or two cryptographic techniques to offer security. The privacy component in the cloud infrastructure is a concern. It offered a way for improving the safety of cloud databases. The benefits offered by this method, which combines several cryptographic algorithms like RSA, 3DES, and arbitrary number generators, occur at the expense of efficiency [9-12].

Several studies concluded that a hybrid method can partially achieve these requirements. A hybrid method of providing data security in the cloud eliminated the disadvantage of Security in RSA, in two stages, and the Feistel Cipher method. Because two methods were utilized in two stages, the likelihood of a man-in-the-middle attack has been lowered. Information is only transmitted across the channel in encoded form, which reduces the risk of disclosing information. This mechanism uses the RSA algorithm and Hash function to offer confidentiality while the information is being transmitted. The two key characteristics that set one encryption algorithm apart from another are its capacity to protect information from attacks and how quickly and effectively it does so. Data transmission across any communication channel may be securely encrypted using both asymmetric and symmetric key techniques. The optimum security algorithm, which will be used in cloud applications to make cloud information safe and impervious to hackers, has been determined as Blowfish, AES, RSA, and DES algorithms.

Researchers presented an evaluation of symmetric and asymmetric techniques with an emphasis on symmetric cryptography for security considerations, including which method should be used for cloud-based software and services that require link data and encryption. The researchers provided a brief comparative analysis and overview of cryptographic techniques, focusing on the symmetric approach that should be used for cloud-based applications and services that require linking data and encryption. The main crucial difference between AES and DES was discussed along with its limitations, logically concluded that AES can be implemented considerably better in high- or low-level programming. Three well-known symmetric key encryption algorithms—Blowfish, AES, and DES—were appropriately compared and evaluated. When evaluating an algorithm's effectiveness in various situations, it was taken into account how the method behaves under multiple data loads. Researchers carried out a study to evaluate the effectiveness in terms of hardware platforms with varying computational power where various file sizes are executed to measure the processing times for every method on various hardware and demonstrated that the AES algorithm outperformed alternative hardware processors in terms of throughput as well as system performance.

2. Cloud Security Issues and Cryptography

Cloud has several complex design concerns that need extensive expertise and have an effect on the reliability and functionality of the entire system. Numerous security concerns consist of [13-15]:

- (a) Data security:** Typically, sensitive information was kept inside the boundary of the organization. However, in the cloud, business information is stored outside the boundaries, necessitating robust encryption.
- (b) Cloud Privacy and Confidentiality:** Confidentiality is the process of preventing the disclosure of confidential data to unapproved systems, individuals, or processes. The location of the unencrypted information in the cloud is known to the provider of the cloud.
- (c) Locating and moving data:** Cloud storage is a black box. Users are never aware of where the information is stored. High levels of information mobility are provided by cloud computing.
- (d) Storage, Backup, and Recovery:** The provider of cloud services assures an appropriate data resilience storage system has been set up whenever clients migrate their information to the cloud. The information will be managed by cloud storage providers in various versions over numerous separate locations.
- (e) Data Integrity:** When information is saved on the cloud, it must be accurate. Data integrity is violated when changes to a data file occur within two updates.

There are several cryptography techniques available to deal with such security challenges. Integrity checking, which assures the message's receiver that it has not changed because it was created by a reliable source, and authenticity is two features that cryptography may offer. By using both encryption and decryption, security objectives are fulfilled. Three kinds of techniques are combined in the process of encryption and decryption.

(1) Symmetric Key: When it comes to encryption, symmetric key cryptography is used when the recipient and the sender both utilize the same key. The same key is employed for both participants in symmetric key cryptography. DES, AES, 3DES, BLOWFISH, etc., are a few examples.

(2) Asymmetric Key: Public key cryptography employs unique keys for encryption and decryption. A private key and a public key are utilized in asymmetric or public key cryptography. The recipient keeps the private key, while the public key is made known to the general public. Examples include RSA, Diffie Hellman, and DSA.

(3) Hash algorithms: A hash function that is used in cryptography is an algorithm that is thought to be virtually hard to reverse, or reproduce the data input only using the hash value. The ‘workhorses of contemporary cryptography’ were referred to as one of these one-way hash algorithms. The hash value is frequently referred to as the message digest or just the digest, while the input data is often referred to as the message. For instance, MD5, SHA, etc. The features, services, and cloud deployment models are displayed in Figure 1.

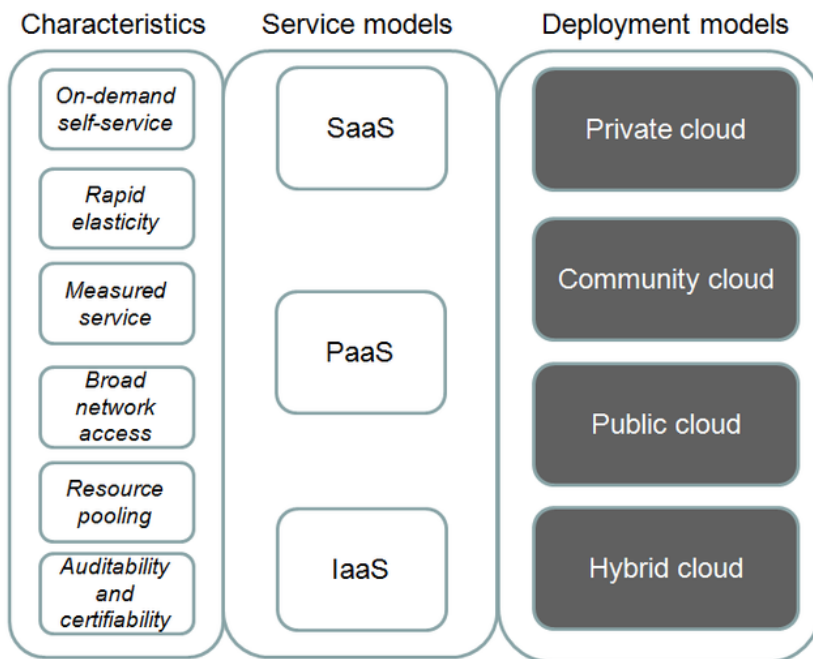


Figure 1. Characteristics, service models, and deployment models

2.1. Characteristics of Cloud

With on-demand self-service, the user has the opportunity to complete their tasks with the assistance of the cloud-based service provider without being interrupted by people. When users have broad network access, they may utilize any platform, including a laptop or a mobile device, to obtain the service.

Resource pooling is the process of making resources accessible in a pool-like framework because many people may access and share them. Rapid elasticity refers to the ability of resources rapidly change in response to demands.

Utilizing quantified services allows both the cloud vendor and the customer to determine how much resource is being utilized by each party and the amount of cloud storage is being consumed for billing.

3. Literature Survey

Data confidentiality in cloud computing with blowfish algorithm - suggests an approach that makes use of cryptography to offer a dependable and simple method for protecting data to address privacy concerns. The

scheduler carries out encryption. After converting plaintext into ciphertext, the ciphered information is sent to the cloud. The information is gathered in plaintext format and saved on the server when it has to be accessed from the cloud. AES, DSA, and Steganography are a few cryptographic methods that are proposed in the work - Triple Security of Data in Cloud Computing. The data is encrypted using AES, Steganography is employed, and DSA is employed for authentication.

The RSA algorithm is being used to offer data privacy in cloud environments, according to -Data Security in Cloud Computing Using RSA Algorithm. Ron Rivest, Adi Shamir, and Len Adleman make up the term RSA. Cryptography using public keys includes RSA. This method incorporates RSA for both encryption and decryption of data. The procedure entails encrypting the data before uploading it to the server.

The required information is retrieved from the cloud, the cloud service provider verifies the identity of the user, and then the data is decrypted. The system is reliable because RSA is employed to grant authenticated access to the designated user alone.

3.1. Types of Cryptography

Two different kinds of cryptographic techniques are present (a) symmetric-key cryptography, and (b) asymmetric-key cryptography.

(a) Operation of Symmetric-Key Cryptography

The same key is utilized for both decryption and encryption in a cryptographic system. The operation of symmetric key cryptography is shown in Figure 2.

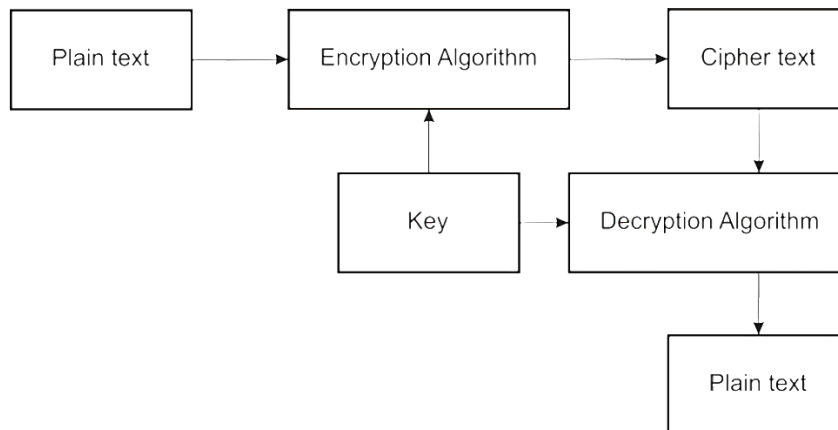


Figure 2. Operation of Symmetric Key Cryptography

DES is a symmetric key-based approach. The Data Encryption Standard (DES), a technique used to protect unencrypted data, was originally released by the National Bureau of Standards of the United States in January 1977. A block cipher that uses 64-bit data blocks is known as DES and is described in FIPS Publication 46-3.

(b) Operation of Asymmetric-Key Cryptography

The encryption and decryption keys of an asymmetric are distinct yet interconnected. The private key is used for decrypting, whereas the public key is used for encrypting. The RSA is an asymmetrical method. The RSA

cryptographic algorithm was created by Rivest, Adi Shamir, and Leonard Adleman at MIT in 1977. In 1978, it was documented. The operation of asymmetric cryptographic algorithms is shown in Figure 3.

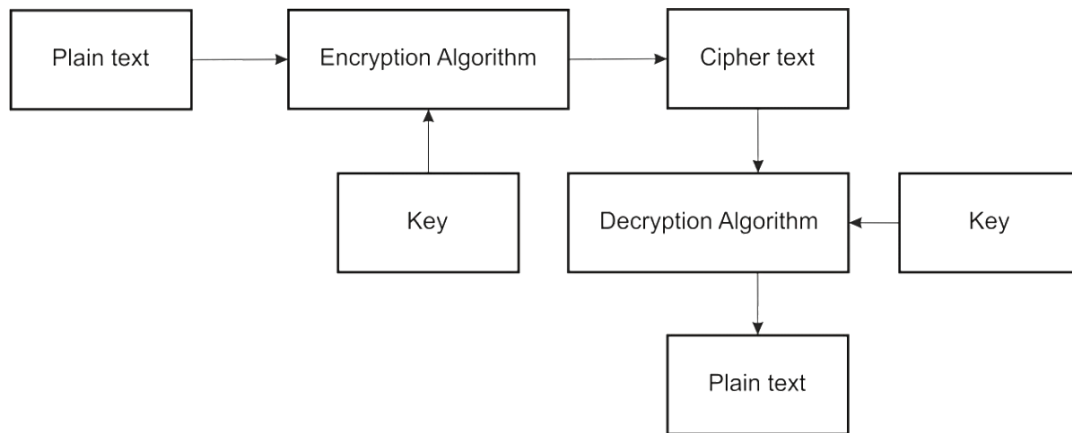


Figure 3. Operation of Asymmetric Key Cryptography

Cloud computing's primary problem is data privacy. The data is encrypted before being sent into the cloud but uses the cryptography approach. For this, RSA and DES are employed. The steps are as follows: 1) Data Preparation, 2) Data Encryption, 3) Data Transfer, as well as 4) Data Processing.

(1) Preparation of Data

The data must initially be processed for the encryption procedure. Information that has been analyzed by an algorithm can be in file form. The major file types are the .txt, .java, and .m. In other words, information must only be shown as text and not as images.

(2) Encryption of Data

Data that has to be sent can be secured using either the RSA or DES techniques once the information has been prepared. At this time, a digital file that is encrypted has been obtained.

(3) Transfer of Data

Encryption is being used widely to solve the risk of sensitive information being revealed while transmitted from one person to another. Therefore, cloud storage and file transfers are encrypted. Accordingly, the original file is not copied elsewhere on the system. Due to this verification, integrity and confidentiality are guaranteed. Cloud computing potentially achieves better data privacy.

(4) Processing of Data

Processing includes all uses and transformations made to the information. The capability of data processing in the encoded format as homomorphic encryption—is still being explored. By using homomorphic encryption, data providers can have the encrypted information analyzed by a different party without concerns that the party will discover whatever the information is in its unencrypted state. Although the researcher Craig Gentry concedes that it could take up to forty years before the idea is put into action, it is a highly interesting concept for the paradigm of cloud computing.

4. Security Algorithms in Cloud Computing

4.1. RSA Algorithm

Named after its developers Rivest, Shamir, and Adleman, the most commonly used Public Key algorithm is RSA. RSA is essentially asymmetric encryption and decryption algorithm. It is asymmetric in that everybody has a copy of the public key that can be utilized to encrypt messages, while only a select few have access to the private key that is utilized to decode messages. Following is an explanation of how RSA will operate in a cloud infrastructure: The RSA technique is employed in cloud technology to guarantee data protection. Information security aims to limit accessibility to only authorized parties who must know about it. Information is then saved in the server after encryption. So that a query to the cloud vendor may be made if it becomes necessary.

Information is given to the user when the cloud vendor authenticates the users. Because RSA is a block cipher, each message is translated into an integer. In the hypothetical cloud infrastructure, the private key is only accessible to the individual who created the data; the key is shared with everybody. As a consequence, the cloud service provider performs encryption, as well as the cloud consumer or user performs decryption. Just the associated Private Key will be used to decode the information after it has been encoded with the Public key.

4.2. AES Algorithm

Data is secured using the Advanced Encryption Standard (AES), commonly referred to as Rijndael. AES is a well-known and commonly used symmetric key encryption that has undergone thorough analysis. For this, the symmetric key encryption technique in AES with a 128-bit key length is applied. According to the implementation application, the client initially selects to utilize online services and migrates his information there.

The client subsequently makes his service requests to a cloud service provider (CSP) and selects the best services the operator has to provide. Information will initially be encoded using the AES technique before being delivered to the provider whenever data migration to the selected CSP takes place and going forward anytime an application uploads any information to the cloud. Information that has been encoded and stored in the cloud will only be accessible upon the user's query once it has been decoded on their end. Nowhere in the clouds is plaintext data ever generated. All information categories are covered by this.

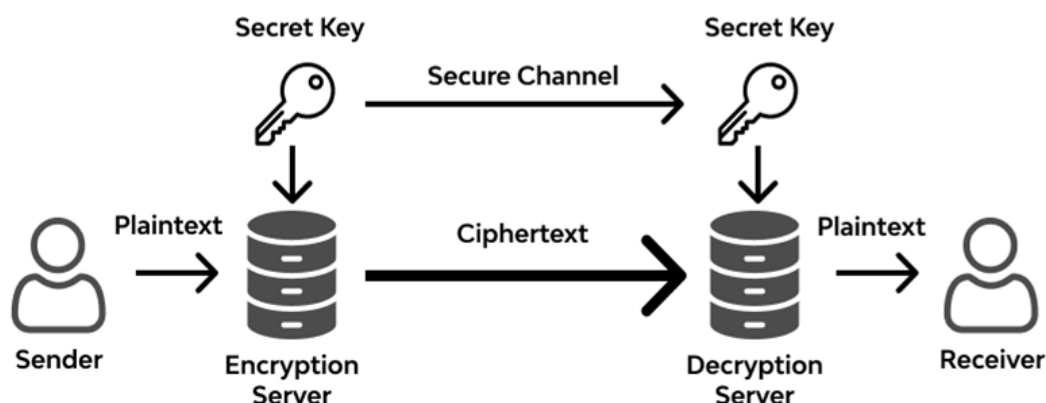


Figure 4. Articulation of AES Algorithm

Despite requiring any modifications to the program, this encryption technology may be rapidly and simply incorporated. The key never is kept with the encrypted files because doing so might compromise the key as well. A physical key management server can be deployed on the recipient's location to keep the keys. Information and keys are protected via encrypting, which also ensures that they stay inside the recipient's control and are not revealed while being stored or transported. For a wide range of applications, AES has taken the place of the DES as the acceptable standard. The AES algorithm's execution is shown in Figure 4.

4.3. DES algorithm

DES is a block cipher, or data encryption standard. The data is encrypted in blocks with 64 bits long. DES receives 64 bits of plaintext as inputs, resulting in 64 bits of ciphertext. Despite a few small exceptions, both decryption and encryption employ an identical algorithm and key. Although a 64-bit key is an actual input, the key length for this algorithm is 56 bits. Hence, DES is a symmetric key algorithm.

4.4. Blowfish Algorithm

The cryptographic technique known as blowfish uses symmetric keys. With a varying key of 128–448 bits, Blowfish encodes 64-bit blocks. The following objectives are considered when creating Blowfish, as per Schneier: (a) On 32-bit CPUs, the fast-Blowfish encryption rate is 26 clock cycles per byte. (b) Blowfish may operate in storage that is as little as 5 kilobytes small. (c) Simple-implementation Blowfish's architecture is straightforward because it only employs simple operations like addition, XOR, and database lookup. (d) The variable key size of Blowfish can be as long as 448 bits, making it also secure and adaptable. Applications in which the key does not change regularly, like communications link encryption, are a better match for blowfish (e.g. Packet Switching).

5. Data integrity

When one refers to database data integrity, one may think that it refers to the absence of any unintentional or intentional change of user information. In other terms, integrity is the guarantee that only legitimate people may obtain or change the information, or might say it is the fundamental method to validate the user's information. The need to protect the integrity of data in cloud computing is very significant. Once information is stored in the cloud, the client completely relies on the service provider to offer dependable services to its users, and they constantly expect that their information is safe. But various kinds of problems might also happen. To reduce storage capacity or maintain less replication than stated, certain cloud providers could be deceitful and destroy data that was not used or is only used sparingly. Despite the data loss, some providers of cloud services could refuse to acknowledge this and insist that the information is still there and in the same manner that the consumer originally placed it. We may thus state that data redundancy can occur at any moment and in any layer of storage. Loss of data can occur for a variety of causes, such as regulator failure, bit corruption, disc breakdown, etc.

In addition to this, information might become damaged while being transferred between locations. In cloud applications, the inclusion of many hardware gadgets may potentially cause data to be lost. Rather than focusing on the problems, cloud technology offers users several advantages that a conventional storage solution provides. We also cannot claim that putting information in the cloud is a poor decision because we can check the information using various protective measures to guarantee data integrity.

This paper elaborates on the techniques and reasons for using cryptographic methods to guarantee the integrity of user information. Security of data is often defined by the company's demands for integrity and confidentiality. Data protection is at risk whenever the end-user has no influence over his or her data and that information is maintained and handled by a third person, that is exactly what occurs in the case of cloud computing.

6. Conclusion

A typical user has a large library of documents that he utilizes for that specific task. Consequently, substantial storage capacity is needed to place these data, making storage as a service one of the crucial services offered by cloud providers. Clients get accessibility to all of these documents anytime they need them. It is, therefore, necessary to maintain those documents appropriately because of the frequent exposure. Because cloud technology outsources information to a distant place, this may provide a serious issue. Moreover, the user is unaware of the security of their information. A user is extremely concerned regarding the information and believes that the cloud is not reliable and sufficient. An analysis of applying cryptographic methods to lessen the integrity issues in cloud computing has been presented in order to comprehend these security concerns.

Declarations

Source of Funding

This research did not receive any grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing Interests Statement

The author declares no competing financial, professional and personal interests.

References

- [1] Q. K. Kadhim, R. Yusof, H. S. Mahdi, S. S. A. Al-Shami, and S. R., Selamat A review study on cloud computing issues, Journal of Physics: Conference Series, vol. 1018, no. 1, p. 012006, 2018.
- [2] V. Agarwal, A. K. Kaushal, and L. Chouhan, A Survey on Cloud Computing Security Issues and Cryptographic Techniques, in Social Networking and Computational Intelligence, Singapore, pp. 119134, 2020.
- [3] H. Abroshan, A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography Algorithms, Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 6, 2021.
- [4] Wei P Wang D Zhao Y Tyagi SK Kumar N., Blockchain data-based cloud data integrity protection mechanism Future Generation Computer Systems.
- [5] Malik A, Om H, Rivera W., Cloud computing and internet of things integration: architecture, applications, issues, and challenges Sustainable cloud and energy services, Springer International Publishing, 2018.
- [6] Munivel E, Kannammal A., New authentication scheme to secure against the phishing attack in the mobile cloud computing. Secur Commun Netw., 45:1–11, 2019.
- [7] Obinna E, Faraz FM, Philipp W, Ramin Y., A JSON token-based authentication and access management schema for cloud SaaS applications. In: The 5th IEEE international conference on future internet of things and cloud (FiCloud), 2017.

- [8] Lee Y, Rathore S, Park JH et al., A blockchain-based smart home gateway architecture for preventing data forgery. *Hum. Cent Comput Inf Sci.*, 10: 9, 2020.
- [9] Ramotsoela DT, Hancke GP, Abu-Mahfouz AM., Attack detection in water distribution systems using machine learning. *Hum Cent Comput Inf. Sci.*, 9: 13, 2019.
- [10] Shailendra R, Vincenzo L, Park JH., SpamSpotter: an efficient spammer detection framework based on intelligent decision support system on facebook. *J Appl Soft Comput.*, 67: 920–932, 2017.
- [11] Shailendra R, Sharma PK, Park JH., XSSClassifier: an efficient XSS attack detection approach based on machine learning classifier on SNSs. *J Inform Process Syst.*, 13(4): 1014–1028, 2017.
- [12] Shailendra R, Park JH., Semi-supervised learning based distributed attack detection framework for IoT. *J Appl Soft Comput.*, 72: 79–89, 2017.
- [13] Siddeeq Y, Shayma W., Firewall and VPN investigation on cloud computing performance. *Int J Comput Sci Eng Survey.*, 5(2): 1–10, 2014.
- [14] Ljubomir MV, Milan DS, Aleksandar S, Zoran DP., Influence of encryption algorithms on power consumption in energy harvesting systems. *J Sens.*, 10: 15–20, 2019.
- [15] Megouache L, Zitouni A, Djoudi M., A new framework of authentication over cloud computing. In: Silhavy R, Silhavy P, Prokopova Z (eds) *Cybernetics approaches in intelligent systems. CoMeSySo 2017. Advances in intelligent systems and computing*, Vol. 661. Springer, Cham, pp. 262–270, 2018.